AIIB Directive on
the Information Classification System
December 21, 2018

1. Overriding Objective

1.1. This Directive establishes the requirements for classifying and handling information of the Asian Infrastructure Investment Bank (the Bank) whilst reconciling the aims of: (a) preventing unauthorized use, disclosure and loss of information; (b) facilitating internal information sharing to enhance operational efficiencies; and (c) maximizing public access to information to promote transparency and accountability.

1.2. The exercise and interpretation of this Directive shall seek to give effect to this Overriding Objective.

2. Related Provisions

2.1. This Directive is related, but without prejudice, to the following provision of the Articles of Agreement:

"Article 47 Immunity of Assets and Archives

1. Property and assets of the Bank, wheresoever located and by whomsoever held, shall be immune from search, requisition, confiscation, expropriation or any other form of taking or foreclosure by executive or legislative action.
2. The archives of the Bank, and, in general, all documents belonging to it, or held by it, shall be inviolable, wheresoever located and by whomsoever held."

2.2. The related provision of the Bank's Policy on Public Information (PPI) is:

"11. Classification of Information. To the extent that the President adopts an internal classification system for information held by the Bank, that system shall be consistent with this Policy and, in particular, adhere to the Governing Principles stated herein."

2.3. The specific related provision of the Directive on Records and Information Management regarding information classification is:

"5.4 Security of Records and Information. The President shall issue a Directive to establish an effective information classification system to ensure the confidentiality, integrity, trustworthiness, availability, and protection of privacy of information. Each Record and information shall be assigned an appropriate security classification based on the nature of the content. Internal access and sharing restrictions shall not be imposed unnecessarily but shall be based on the associated classification of information. As a general rule, information is a resource to which all Bank Personnel shall have access, except where the nature of the information requires restriction. While the Bank shall make every effort to maximize access, Records and information that contain sensitive content shall be protected against unauthorized access. Disclosure and public access to Records and information outside the Bank shall be governed by the Bank's policy on disclosure of public information and its related directive(s) and administrative guidance."

2.4. The specific related provisions of the Directive on Information Technology Security for Bank Personnel are:

"4.9 Restricted Data: Data that contains information which is defined as Restricted under the Directive that establishes the Bank's security of information classification."

"E. Computing and Storage Devices Use
5.5 When using removable storage media, including optical media and USB flash drives, Bank Personnel shall use encryption for files that contain Restricted Data.
5.6 Bank Personnel shall delete Restricted Data from their devices when the data is no longer required by them for official Bank purposes."

"G. Network Use and Email Use.
7.5 When communicating or sharing Restricted Data over any network, Bank Personnel shall only use systems and tools that have been approved by the Manager, IT Division or the Vice President and Chief Administrative Officer (VP & CAO), and shall use encryption to protect the security of such data."

3. The Information Classification System Imperatives

3.1. The Information Classification System aims to protect the confidentiality, integrity and availability of information according to category levels as follows:

Confidentiality. Ensures information is not accessed by or disclosed to unauthorized individuals and entities. This also ensures the means for protecting personal data, privacy and proprietary information.

Integrity. Protects against unauthorized modification or destruction of information.

Availability. Ensures timely and reliable access to and use of information for authorized users.

4. General Principles

4.1. In accordance with the Policy on Public Information, disclosure of and access to information shall promote the greatest possible access to public information. Internal access and sharing restrictions shall not be imposed unnecessarily and shall be based on the associated classification of information.

4.2. Information is a resource to which all Bank Personnel shall have access to, except where the nature of the information requires restriction.

4.3. While the Bank shall make every effort to maximize access, information that contains sensitive content shall be protected against unauthorized disclosure and access. Access to restricted information shall be granted on a *Need to Know* basis.

4.4. All information that the Bank creates, receives, stores, and processes shall be classified according to the sensitivity of the content and the risks associated with unauthorized disclosure and access.

4.5. The information classification rules shall be applied throughout the lifecycle of information, namely creation, use, storage and disposition (destruction or archiving) and for all media on which the information reside regardless of the format (electronic or physical).

4.6. This Directive applies to all Bank Personnel, including in their interactions with Board Officials. However, this Directive does not extend to Board Officials including in their handling, distribution, storage and maintenance of information obtained in the performance of their duties as Board Officials. Board Officials shall comply with the Code of Conduct for Board Officials in respect to the disclosure of information.

5. Definitions

5.1. **Bank Personnel.** As defined in the Code of Conduct for Bank Personnel.

5.2. **Bank Premises.** As defined in the Directive on Security and Safety: Part 5: Security of Bank Premises.

5.3. **Business Units.** As defined in the Directive on Business Continuity.

5.4. **Declassification.** Declassification means a change of classification of Sensitive Information after formal approval from the Information Originator or Owner.

5.5. **Documents.** As defined in the Directive on Records and Information Management (RIM).

5.6. **Information.** As defined in the Policy on Public Information.

5.7. **Information Originator or Owner.** Bank Personnel who create or receive the information in the course of their official duties for the Bank.

5.8. **Need to Know.** A requirement for accessing information by Bank Personnel to perform tasks or services to fulfil their official duties.

5.9. **Sensitive Information.** Contrary to publicly available information, Sensitive Information is information that requires protection through disclosure restrictions as unauthorized access to such information may adversely affect the Bank operations, assets or Bank Personnel.

5.10. **Official Channels.** Any Bank-owned platform or publication in both digital and print formats. This includes, but is not limited to, AIIB's website, social media accounts and Records Management System.

6. Information Classification System

6.1. The appropriate use of and security measures to protect information are dependent upon the determined classification based on the level of sensitivity of content as defined below. The Bank classifies all information into one of the four following categories.

Table 1: Information Classification System Table

Category Levels	Security Classification	Description
Category-I	**PUBLIC**	Disclosure of such information will not have any implication on the operation or reputation of the Bank or the clients of the Bank. Information in this category can be made public through Official Channels.
Category-II	**OFFICIAL USE ONLY**	Information used for the day-to-day administration and operation of the Bank including internal communications intended for Bank Personnel. Information in this category has not been approved for public disclosure yet and may or may not contain Sensitive Information. Public disclosure of such information may cause minor harm on the operation or reputation of the Bank or the clients of the Bank.
Category-III	**RESTRICTED**	Restricted information contains content that, for one or more reasons, may only be disclosed to or accessed by authorized individuals or groups only. Unauthorized disclosure of or access to such information (internally and externally) may cause significant harm on the operation or reputation of the Bank or the clients of the Bank. Information in this category is restricted at the time of its creation but may become eligible for disclosure over time when the sensitivity of the content no longer exists.
Category-IV	**STRICTLY CONFIDENTIAL**	Information that is deemed extremely sensitive which requires the highest degree of access control and security protection. Any unauthorized disclosure of or access to such information (internally and externally) is likely to cause severe harm on the operation or reputation of the Bank or the clients of the Bank or may result in legal action against the Bank. Information in this category shall never be eligible for declassification or public disclosure due to its highly sensitive nature.

6.2. In cases where information may fall into more than one classification, the highest applicable restriction of classification shall apply. To promote maximum disclosure and transparency, Bank Personnel may consider redacting sensitive information in documents to allow for public disclosure.

6.3. Information received from a third party shall be classified as STRICTLY CONFIDENTIAL if the information is being provided in confidence or the information received by the Bank has not been classified by such third party.

6.4. Information relating to Bank Personnel's personal use of the Bank's computer systems, electronic devices and internet access undertaken in a manner consistent with the Code of Conduct for Bank Personnel does not fall within the scope of this Directive.

7. Rules on Information Classification

7.1. **Default Classification for Bank Documents.** The default information classification for all Documents of the Bank is category II – OFFICIAL USE ONLY. In the absence of any explicit data classification labels, all Bank Documents shall be presumed to be in this category. All information within the Bank shall be deemed to be accessible by Bank Personnel if it contains information they Need to Know to conduct their business functions.

7.2. **Declassification of Information.** Certain information classified RESTRICTED may be eligible for declassification for access and disclosure purpose over the time once the sensitivity of content has diminished. Information created or received by the Bank shall be declassified in accordance with the declassification schedules in the Administrative Guidance on Information Classification System. The Records and Information Management Section of the Facilities and Administrative Services Department, in consultation with the Head of Communications and Development and the relevant Information Owner or Originator shall determine whether information is eligible for declassification in accordance with the Administrative Guidance on Information Classification System.

7.3. **Requirements for Classification Marking.** At a minimum, Sensitive Information shall be labelled so users are aware of the classification of the information and may handle or release it appropriately according to the Administrative Guidance on Information Classification System. Classification labels may be a water mark on an electronic document, stamp on a hardcopy document or any other ways to identify the category of information content on a specific media.

7.4. **Requirements for Handling Distribution, Storage and Maintenance.** Business Units and Bank Personnel shall handle information according to the classification of information. RESTRICTED and STRICTLY CONFIDENTIAL information shall only be stored on Bank authorized media and devices. Access to such Sensitive Information shall be limited to authorized individuals only. Sensitive Information shall not be distributed or sent without the appropriate classification labels.

7.5. **Methods of Destruction of Information.** All information shall be destroyed under confidential conditions, unless it is already publicly available. Where information is approved and eligible for destruction, this shall be undertaken by methods appropriate to the information sensitivity. Information classified RESTRICTED and STRICTLY CONFIDENTIAL shall be disposed of in such a manner that the information cannot be reconstructed. If Bank Personnel are uncertain of the status of an information content, it

should be treated as STRICTLY CONFIDENTIAL and destroyed under confidential conditions.

8. Responsibilities

8.1. **Bank Personnel** shall adhere to the Bank's Information Classification System and identify the appropriate security measures of information under their custody. The Information Originator or Owner shall assess and assign the classification level to information. They shall then apply the appropriate control measures to protect that information as specified in this Directive and the Administrative Guidance on Information Classification System.

8.2. **Heads of the Business Units** shall ensure Bank Personnel they manage adhere to this Directive and the Administrative Guidance on Information Classification System.

8.3. **Records and Information Management Unit** of the Facilities and Administrative Services Department shall be entrusted with the overall responsibility for implementing the Bank's Information Classification System.

8.4. **Information Technology Division** shall be responsible for providing Bank Personnel with information technology infrastructure, mechanisms or instruction for protecting information while it is resident on any Bank-owned or controlled system.

8.5. **Internal Audit Office** may conduct information security and data management audits in accordance with its Terms of Reference.

9. Misconduct

9.1. A breach by Bank Personnel of the terms of this Directive may amount to misconduct under the Code of Conduct for Bank Personnel.

10. Public Information Disclosure

10.1. The PPI and its related Directive and Administrative Guidance governs the disclosure of all information in the Bank's possession. In the event of a conflict between this Directive and the PPI, the Policy and its related Directive shall prevail.

11. Implementation

11.1. The Vice President and Chief Administration Officer shall oversee this Directive and introduce any related Administrative Guidance and ensure its efficient and accurate implementation.

12. Authority

12.1. The Vice President and Chief Administration Officer shall make all final decisions regarding the application of this Directive except in relation to the sharing of information with Board Officials. In respect to the sharing of information by Bank Personnel with Board Officials, the Vice President and Corporate Secretary shall, in consultation with the Vice President and Chief Administration Officer, make all final decisions regarding the application of this Directive.

*****